



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08335207 A**

(43) Date of publication of application: 17.12.96

(51) Int. Cl. **G06F 15/00**
G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12
H04L 9/32

(21) Application number: **07140291**(22) Date of filing: **07.06.95**(71) Applicant: **HITACHI LTD**

(72) Inventor: **ARAI MASATO**
ITO HIROMICHI
ITOU HISAYA

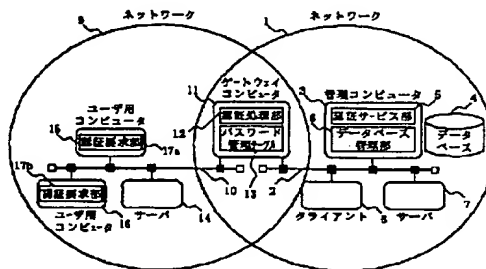
(54) **AUTHORIZING METHOD FOR NETWORK USER**

COPYRIGHT: (C)1996,JPO

(57) Abstract:

PURPOSE: To exclude an illegal gateway computer by ciphering a cipher key with another cipher key by an administration computer before a log-in processing for a user and then distributing the ciphered key.

CONSTITUTION: The user of a network 1 sends an authorization request and his user ID to the administration computer 3 when logging in the network 1. The administration computer 3 when receiving them returns a log-in certificate ciphered with the password of the user and the cipher key to the client 8 that the user uses. On the side of the client 8, the log-in certificate and cipher key are ciphered with the password that the user inputs. Consequently, when the user inputs the correct password at the time of logging-in operation, the user can obtain the log-in certificate and cipher key and utilize resources of the network 1 thereafter by using them. An illegal user who knows no password, on the other hand, can decipher no log-in certificate and cipher key and is unable to use the resources of the network 1.



(11)特許出願公開番号

特開平8-335207

(43)公開日 平成8年(1996)12月17日

(S1)Int.Cl. ^a	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 A
G 0 9 C 1/00		7259-5J	G 0 9 C 1/00	
H 0 4 L 9/00			H 0 4 L 9/00	Z
				A

審査請求 未請求 請求項の数 6 O L (全 9 頁) 最終頁に続く

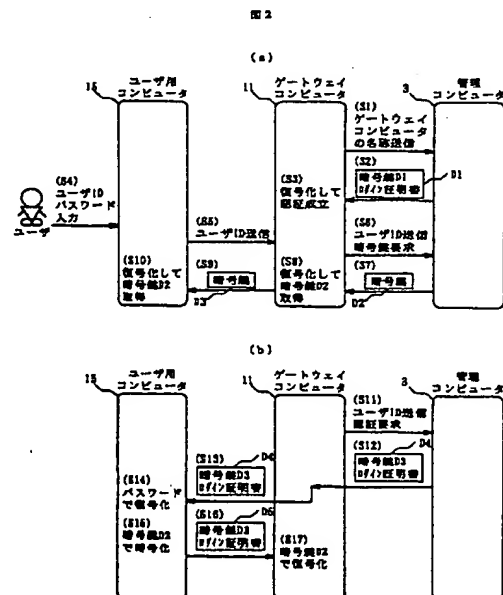
(21)出願番号	特願平7-140291	(71)出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22)出願日	平成7年(1995)6月7日	(72)発明者	荒井 正人 神奈川県川崎市麻生区王禅寺1099番地株式 会社日立製作所システム開発研究所内
		(72)発明者	伊藤 浩道 神奈川県川崎市麻生区王禅寺1099番地株式 会社日立製作所システム開発研究所内
		(72)発明者	伊藤 寿哉 神奈川県横浜市戸塚区戸塚町5030番地株式 会社日立製作所ソフトウェア開発本部内
		(74)代理人	弁理士 小川 勝男

(54) 【発明の名称】 ネットワークユーザ認証方法

(57) 【要約】

【構成】ユーザ認証手段を有する管理計算機とユーザ用計算機とを、ゲートウェイ計算機を介して接続し、ユーザ用計算機から、管理計算機にログインする場合、先ず管理計算機がゲートウェイ計算機とユーザ用計算機のみ共通の暗号鍵D2を配布する(S1~S10)。暗号鍵D2はそれぞれ正当なゲートウェイ計算機とユーザだけが知っている鍵により暗号化された形で渡される。次に、管理計算機がユーザのパスワードで暗号化されたログイン証明書D4を作成し、ゲートウェイ計算機を介してユーザ用計算機に送信する(S1)。ユーザが入力したパスワードでこれを復号化し(S14)、ゲートウェイ計算機に送信する。

【効果】パスワードを通信媒体上に流さずに他のネットワークへログインでき、不正なゲートウェイ計算機を排除でき、セキュリティの面で優れた統合ネットワークの利用ができる。



【特許請求の範囲】

【請求項1】 ユーザおよびコンピュータの名称やパスワードなどの情報を管理するデータベースを有する管理コンピュータと、ユーザが操作するためのユーザ用コンピュータと、前記ユーザ用コンピュータから前記管理コンピュータへのゲートウェイとなるゲートウェイコンピュータとが、通信媒体を介して物理的・論理的に接続されたコンピュータネットワークシステムのネットワークユーザ認証方法であって、前記ゲートウェイコンピュータは、前記データベースに登録されており、前記ゲートウェイコンピュータの名称を前記管理コンピュータに送信するプロセスと、前記ゲートウェイコンピュータから送られた名称に基づいて、前記管理コンピュータが、前記データベースを検索し、前記名称が登録されている場合は、認証に必要なログイン証明書と暗号鍵D1を作成して前記ゲートウェイコンピュータのパスワードにより暗号化し、前記ゲートウェイコンピュータに送信するプロセスと、前記ゲートウェイコンピュータが、暗号化された前記ログイン証明書と暗号鍵D1を自己のパスワードによって復号化するプロセスと、ユーザが前記ネットワークの利用を開始する際に、ユーザ用コンピュータから入力したユーザ名を前記ゲートウェイコンピュータに送信するプロセスと、前記ゲートウェイコンピュータが、前記ユーザ名を前記管理コンピュータに送信するプロセスと、前記ゲートウェイコンピュータから送られたユーザ名に基づいて、前記管理コンピュータが、前記データベースを検索し、前記ユーザ名が登録されている場合は、認証に必要なログイン証明書と暗号鍵D3を作成して前記ユーザのパスワードにより暗号化し、前記ゲートウェイコンピュータに送信するプロセスと、暗号化された前記ログイン証明書と暗号鍵D3を、前記ゲートウェイコンピュータが前記ユーザ用コンピュータに送信するプロセスと、前記ユーザ用コンピュータと、前記ゲートウェイコンピュータは共通の暗号鍵D2を所有しており、前記ユーザ用コンピュータが、前記ユーザが入力したパスワードにより前記ログイン証明書と暗号鍵D3を復号化し、復号できたか否かによって前記ユーザの認証を行い、復号された前記ログイン証明書と暗号鍵D3を、前記暗号鍵D2で暗号化して、前記ゲートウェイコンピュータに送信するプロセスと、前記ゲートウェイコンピュータが、前記ログイン証明書と暗号鍵D3を、暗号鍵D2で復号化して所有するプロセスを備えることを特徴とするネットワークユーザ認証方法。

【請求項2】 請求項1において、前記管理コンピュータが、暗号鍵D2と、暗号鍵D2をユーザのパスワードで暗号化したものとを併せて暗号鍵D1で暗号化したデータを、前記ゲートウェイコンピュータに送信するプロセスと、前記ゲートウェイコンピュータが、暗号鍵D1によりデータを復号化することにより暗号鍵D2を取得し、前記

ユーザのパスワードで暗号化した暗号鍵D2を前記ユーザ用コンピュータに送信するプロセスと、前記ユーザ用コンピュータが、ユーザの入力したパスワードで復号化して暗号鍵D2を取得するプロセスを備えることで、身元の正しいユーザおよびゲートウェイコンピュータのみが共通の暗号鍵D2を取得できるネットワークユーザ認証方法。

【請求項3】 請求項1または請求項2において、前記ユーザ用コンピュータから、前記暗号鍵D2によりゲートウェイコンピュータの正当性を確認し、パスワードを通信媒体上に流さずに、前記管理コンピュータによる認証処理を行うネットワークユーザ認証方法。

【請求項4】 請求項1に記載の前記管理コンピュータと、ファイル操作など各種処理を依頼する役割を持つ一つ以上のクライアントと、前記クライアントからの依頼を受けて処理を実行する役割を持つ一つ以上の第一サーバとを、第一の通信媒体に物理的・論理的に接続して構成されたネットワーク1と、

前記ユーザ用コンピュータと、前記ユーザ用コンピュータからの依頼を受けて処理を実行する役割を持つ一つ以上の第二のサーバとを、第二の通信媒体に物理的・論理的に接続して構成されたネットワーク9を前記ゲートウェイコンピュータを介して接続した統合ネットワーク。

【請求項5】 請求項1に記載の前記管理コンピュータと、ファイル操作など各種処理を依頼する役割を持つ一つ以上の第一クライアントと、前記第一クライアントからの依頼を受けて処理を実行する役割を持つ一つ以上の第一サーバとを、第一の通信媒体に物理的・論理的に接続して構成されたネットワーク1と、ファイル操作など各種処理を依頼する役割を持つ一つ以上の第二クライアントと、前記第二クライアントからの依頼を受けて処理を実行する役割と、前記ユーザ用コンピュータと同じ役割を持つ一つ以上の第二サーバとを、第二の通信媒体に物理的・論理的に接続して構成されたネットワーク9を、前記ゲートウェイコンピュータを介して接続し、前記第二サーバは、ネットワーク9とネットワーク1におけるユーザの名称とパスワードの対応付けを管理するパスワード管理テーブルと、ネットワーク9のユーザを認証する認証手段とを有し、前記認証手段により認証されたユーザについて、前記パスワード管理テーブルから、ネットワーク1におけるユーザの名称とパスワードを取り出して、ネットワーク1への認証処理を行うよう構成された統合ネットワーク。

【請求項6】 請求項4または請求項5において、ユーザが同時に異なる複数のネットワークへ認証されるように作用するネットワークユーザ認証方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はネットワークユーザ認証

方法に関する。

【0002】

【従来の技術】近年、サービスを提供する機能を持つコンピュータと、これらにサービスを依頼する機能を持つコンピュータを相互に接続することで処理の分業化を図るコンピュータネットワークが企業などに導入されている。この方式は、処理依頼とサービス提供という観点からクライアント・サーバモデルと呼ばれる。

【0003】今後更にコンピュータネットワークが普及するにつれて、多種多様なネットワークが共存し、それらを相互に接続することにより各ネットワークの資源を利用する統合ネットワークの必要性が高まることが予想される。

【0004】統合ネットワークの形態の一つとして、図1に示すようにゲートウェイコンピュータを介して各ネットワークを相互にアクセスするものがある。このような統合ネットワークの資源を利用するために、ユーザは接続された各ネットワーク中のユーザ認証機能を有するサーバに対して自分の身元の正当性を証明する必要がある。この動作をログインと呼ぶ。多くの場合、ユーザはサーバに対してパスワードを提供することにより自分の身元を証明する。

【0005】図1において、ユーザはネットワーク9のユーザ用コンピュータ15～16からネットワーク1へログインする際に、ゲートウェイコンピュータ11を介することとなる。このような2階層以上のネットワークにおけるセキュリティに関する発明は、特開平2-16669号公報の「セキュリティ方式」がある。「セキュリティ方式」は、ユーザが入力した各ノードへのパスワードを、直接のアクセス先となるノード（本発明におけるゲートウェイコンピュータに相当する）に送信し、ノードがパスワードをチェックすることで他のノードへのアクセス権の有無を判断する方式である。

【0006】また、ネットワークログインの方式は、特開平5-35678号公報の「ユーザ認証方式」のように、パスワードの機密性を高めるために、パスワードを通信媒体上に流さずにログイン可能とする方式がある。

【0007】

【発明が解決しようとする課題】このように、ゲートウェイコンピュータを介して各ネットワークの資源にアクセスする統合ネットワークにおいて、ユーザはネットワークの資源を利用する前に、必ずゲートウェイコンピュータを介して他のネットワークへログインすることとなる。このとき、ゲートウェイコンピュータが悪意をもったユーザにより仕組まれたものである場合、ゲートウェイコンピュータによって他のユーザのパスワードが盗まれたり、データが破壊される危険がある。しかし、「セキュリティ方式」はパスワードの送信先となるノード（本発明におけるゲートウェイコンピュータに相当する）の正当性をチェックする手段がないため、不正なノ

ードを除外できないという問題がある。

【0008】更に、図1におけるネットワーク1が「ユーザ認証方式」のようにパスワードを通信媒体上に送信せずにログイン可能とするネットワークであるとする。この場合、ネットワーク1のセキュリティレベルを保持するためには、ユーザがネットワーク9からゲートウェイコンピュータを介してネットワーク1にログインする際にもパスワードを送信しないことが望ましい。しかし、「ユーザ認証方式」では、他のネットワークからゲートウェイコンピュータを介してログインする場合のパスワード機密保持については記述されていない。

【0009】本発明の目的は、ゲートウェイコンピュータを介して各ネットワークの資源にアクセスする統合ネットワークにおいて、先ずゲートウェイコンピュータの正当性を確認した上で、ユーザのパスワードを通信媒体上に流さずに他のネットワークへログインする方式を提供することにある。

【0010】

【課題を解決するための手段および作用】本発明は、ゲートウェイコンピュータを介して、ユーザが使用するユーザ用コンピュータと、ネットワーク内のコンピュータやユーザの名称およびパスワードが登録されたデータベースを有する管理コンピュータとを接続した統合ネットワークにおいて、ゲートウェイコンピュータは自己のパスワードを登録したパスワード管理テーブルを有しており、ユーザがログインする前にゲートウェイコンピュータが管理コンピュータから暗号鍵D1をゲートウェイコンピュータのパスワードで暗号化された形で取得するプロセスと、ゲートウェイコンピュータが自己のパスワードをパスワード管理テーブルから読み出して暗号鍵D1を復号化するプロセスと、ユーザがログイン要求を出したときに管理コンピュータが暗号鍵D2を暗号鍵D1で暗号化したデータと、暗号鍵D2をユーザのパスワードで暗号化したデータをゲートウェイコンピュータに配布するプロセスと、ゲートウェイコンピュータが暗号鍵D1で暗号化された暗号鍵D2を復号すると共に、ユーザのパスワードで暗号化された暗号鍵D2をユーザが使用するユーザ用コンピュータに配布するプロセスと、ユーザ用コンピュータがユーザの入力したパスワードで暗号鍵D2を復号化するプロセスによりゲートウェイコンピュータとユーザ用コンピュータに共通の暗号鍵D2を配布し、次にゲートウェイコンピュータが管理コンピュータに対してユーザのログイン要求を提示するプロセスと、管理コンピュータがデータベースを検索し、ユーザ名が登録されている場合は、認証に必要なログイン証明書と暗号鍵D3を作成してユーザのパスワードにより暗号化し、ゲートウェイコンピュータに送信するプロセスと、暗号化されたログイン証明書と暗号鍵D3を、ゲートウェイコンピュータがユーザ用コンピュータに送信するプロセスと、ユーザ用コンピュータがユーザの入力し

たパスワードによりログイン証明書と暗号鍵D3を復号化するプロセスと、ログイン証明書と暗号鍵D3を暗号鍵D2により暗号化してゲートウェイコンピュータに送信するプロセスと、ゲートウェイコンピュータが暗号鍵D2によりログイン証明書と暗号鍵D3を復号化するプロセスを具備することを特徴とするネットワークユーザ認証方法である。

【0011】本発明のネットワークユーザ認証方法では、ユーザのログイン処理の前に、管理コンピュータが暗号鍵D2を暗号鍵D1で暗号化してからゲートウェイコンピュータに配布するので、正当なゲートウェイコンピュータのみが暗号鍵D2を復号化できる。一方、ユーザ用コンピュータには暗号鍵D2をユーザのパスワードで暗号化した形で配布するので、正当なユーザのみが暗号鍵D2を復号化できる。

【0012】次に、管理コンピュータから配布されたログイン証明書と暗号鍵D3を、ユーザ用コンピュータでユーザが入力したパスワードで復号化することで、ユーザのパスワードがネットワークの回線を流れることはない。また、復号化したログイン証明書と暗号鍵D3は、ユーザ用コンピュータにおいて暗号鍵D2により暗号化されてゲートウェイコンピュータに送信されるため、暗号鍵D2を知らない第三者に盗まれる危険がない。

【0013】

【実施例】以下、本発明の実施例を図面を参照しながら説明する。図1は本発明の一実施例として、互いに独立に管理される二つのネットワーク環境を、ゲートウェイコンピュータ11を用いて接続する場合の構成例を示す図である。

【0014】図1において、後述する各要素で構成されるネットワーク1、ネットワーク2を構成する各要素

(後述)間を物理的・論理的に接続し、各種データ転送の媒体となる通信媒体、3はネットワーク1を構成する各要素やユーザの認証処理を専門に行う管理コンピュータ、4はネットワーク1の各要素やユーザに関する情報(ID、パスワード等)を管理するためのデータベース、5はネットワークの各要素やユーザからの要求に応じて、暗号鍵やログイン証明書を要求元に与える認証サービス部、6はデータベースからデータの読み出しや書き込みを行うデータベース管理部、7はクライアント8からの要求に応じて各種サービスを提供するサーバ、8はネットワーク1のユーザにコマンドインタフェースやアプリケーションプログラムを提供し、それらを通じてユーザから発せられる要求に応じて、管理コンピュータやサーバ7と通信を行うクライアント、9はネットワーク1とは独立に管理され、後述する各要素で構成されるネットワーク9、10はネットワーク9内の後述する各要素間を物理的・論理的に接続し、各種データ転送の媒体となる通信媒体、11は通信媒体2および通信媒体10に接続され、後述するユーザ用コンピュータ15~1

6からのコマンドをネットワーク1に送信し、結果をユーザ用コンピュータに返送する役割をもつゲートウェイコンピュータ、12は管理コンピュータに認証要求を送信してネットワーク1へのログイン処理を行う認証処理部、13はゲートウェイコンピュータおよびネットワーク9のユーザに関する情報(IDやパスワード等)を管理するパスワード管理テーブル、14は後述するユーザ用コンピュータ15~16からの要求に応じて各種サービスを提供するサーバ、15~16はネットワーク9のユーザにコマンドインタフェースやアプリケーションプログラムを提供し、それらを通じてユーザから発せられる要求に応じて、ゲートウェイコンピュータ11やサーバ14と通信を行うユーザ用コンピュータであり、それぞれユーザのIDやパスワードを入力する認証要求部17aと17bを備えている。

【0015】ネットワーク1及びネットワーク9は、それぞれ単独での運用が可能になっている。単独の運用での動作を簡単に説明する。

【0016】複数のコンピュータが接続され、各々のコンピュータが管理する資源を、他のコンピュータからも利用できるように構成されたネットワークシステムでは、ユーザはネットワークの資源を利用する前に自分の身元を証明するためのログイン動作を行わなければならない。一般的にログインとは、ユーザIDと呼ばれるユーザの識別子と、パスワードなどユーザ本人のみが持つ情報を示すことで、ネットワークシステムに対して自分が正規のネットワークユーザであることを証明するための手続き(これを認証という)である。

【0017】本実施例におけるネットワーク1は、ネットワーク内にユーザ認証処理を専門とする管理コンピュータ3を有している。ネットワーク1のすべてのユーザは、ログイン時にこの管理コンピュータ3に対して認証要求とユーザIDを送信する。管理コンピュータ3はログイン要求を受けると、ユーザのパスワードで暗号化したログイン証明書と暗号鍵をユーザが使用するクライアントに返す。ログイン証明書は、ユーザがネットワーク1の資源を利用する際に、自分の身元を証明するために必要なものである。一方、暗号鍵は管理コンピュータ3と送受信するデータを暗号化復号化するために必要なものである。クライアント側では、ユーザが入力したパスワードによりこのログイン証明書と暗号鍵を復号化する。つまり、ユーザが正しいパスワードを入力すればログイン証明書と暗号鍵を入手でき、以後ユーザはそれらを用いてネットワーク1の資源を利用できるようになる。反対にパスワードを知らない不正なユーザはログイン証明書と暗号鍵を復号化できないため、ネットワーク1の資源を利用できないことになる。以上のようにネットワーク1では、ログイン時にユーザのパスワードが通信媒体2に流れないという特徴がある。

【0018】一方、本実施例におけるネットワーク9で

10

20

30

40

50

は、ネットワーク内の全てのサーバがユーザ認証手段とユーザの暗号化されたパスワードを管理する手段を有している。ログイン時には、例えばユーザ用コンピュータ15ではユーザが入力したパスワードを暗号化して、ユーザIDと併せてサーバに送信する。このときパスワードの暗号化に使用する鍵は常に固定なものとする。サーバはクセイアントから受信したユーザの暗号化パスワードを、サーバ自身が管理する暗号化パスワードと照合する。両者が一致していれば、サーバが管理するネットワークの資源に対してアクセスを許可する。反対に、両者が一致しなければアクセスを許可しない。

【0019】図2の(a)と(b)は、ネットワーク1に登録されているユーザが、本発明のネットワークユーザ認証方法により、ユーザ用コンピュータ15からネットワーク1にログインする処理を示したものである。図2(a)は、ユーザのログイン処理に先立ってユーザ用コンピュータ15からゲートウェイコンピュータ11の正当性を確認するための手順を示している。同図に示すように、

(S1)ゲートウェイコンピュータの認証処理部12は、起動時にゲートウェイコンピュータ自身の名称を管理コンピュータ3に送信し、認証要求を出す。

【0020】(S2)管理コンピュータ3は、暗号鍵1とログイン証明書を作成し、これをゲートウェイコンピュータのパスワードで暗号化したデータD1を送信する。データD1の構造を図3(a)に示す。図3において、31は暗号鍵であり、32はログイン証明書である。33は暗号鍵31とログイン証明書32を認証要求元であるゲートウェイコンピュータのパスワードで暗号化していることを表す。また、ゲートウェイコンピュータのパスワードは、データベース4で管理されており、認証サービス部5がデータベース管理部6を通じて読み出す。図4に、データベース4で管理される情報の一例を示す。管理コンピュータ3は、例えば、立ち入り制限のある安全な部屋に配置され、ネットワーク1の管理者のみがデータベース4にアクセス可能とすることで、パスワードの機密保護を行う。

【0021】(S3)認証処理部12は、パスワード管理テーブル13からゲートウェイコンピュータのパスワードを取り出してデータD1を復号化し、ログイン証明書と暗号鍵をパスワード管理テーブル13に登録する。これにより、正当なゲートウェイコンピュータだけが暗号鍵とログイン証明書を取得でき、管理コンピュータにより認証されたこととなる。図5にパスワード管理テーブル13で管理される情報の一例を示す。同図に示すように、パスワード管理テーブル13には、ネットワーク1におけるユーザ及びゲートウェイコンピュータ自身のIDとパスワードの他に、ネットワーク1におけるログイン証明書と暗号鍵が登録されている。ログイン証明書と暗号鍵は、ネットワーク1にログインしている間のみ登

録される。また、パスワード管理テーブル13は、ネットワーク9の管理者のみがアクセス可能とすることで、パスワードやログイン証明書および暗号鍵の機密保護を行う。

【0022】(S4)ユーザは、認証要求部17aからユーザIDとパスワードを入力する。

【0023】(S5)認証要求部17aは、ゲートウェイコンピュータにユーザIDを送信する。

【0024】(S6)認証処理部12は、管理コンピュータにユーザIDを送信し、ユーザ用コンピュータ15とゲートウェイコンピュータ11との間で使う暗号鍵を要求する。

【0025】(S7)認証サービス部5は暗号機2を作成し、ゲートウェイコンピュータに送信する。このとき、送信データD2は図3(b)に示すような構造になっている。図3(b)において、34は暗号鍵D2であり、35は暗号鍵D2をユーザのパスワードで暗号化したデータである。また、36は暗号鍵34と35のデータを暗号鍵で暗号化したデータを表す。

【0026】(S8)認証処理部12は、(S3)で取得した暗号鍵D1によりデータD2を復号化し、暗号鍵D2とデータD3を取得する。データD3は図3(b)における35のデータに相当する。このとき、ゲートウェイコンピュータが暗号鍵D1を知らなければ暗号鍵D2とデータD3は取得できない。言い換えれば、暗号鍵D2とデータD3を取得したことは、管理コンピュータ3によって認証されていることを意味する。

【0027】(S9)認証処理部12は、データD3をユーザ用コンピュータ15へ送信する。

【0028】(S10)認証要求部17aは、データD3をユーザが入力したパスワードで復号化し、暗号鍵D2を取得する。ここで、ユーザのパスワードを知っているのは、ユーザ本人と管理コンピュータだけである。つまり、データD3を作成したのは管理コンピュータであり、不正なゲートウェイコンピュータが偽造することはあり得ない。また、ゲートウェイコンピュータが管理コンピュータからデータD3を取得するには暗号鍵1を必要とする。ゲートウェイコンピュータが暗号鍵1を所有していることは、管理コンピュータ3により認証されている、つまり正当なゲートウェイコンピュータであることが証明される。

【0029】以上により、正当なゲートウェイコンピュータとユーザ用コンピュータ15のみに共通の暗号鍵2が配布される。以後、暗号鍵2によって暗号化されたデータを交換することにより、ユーザ用コンピュータ15とゲートウェイコンピュータ11が互いの正当性を確認できる。

【0030】次に図2(b)は、ゲートウェイコンピュータ11が正当なものであることを確認した上で、ユーザがネットワーク1へログインするまでの手順を示して

いる。

【0031】同図に示すように、

(S11) 認証処理部12は、ユーザIDを送信して、ユーザ認証を要求する。

【0032】(S12) 認証サービス部5は、暗号鍵D3とログイン証明書を作成し、これをユーザのパスワードで暗号化したデータD4を送信する。データD4の構造は、前述の図3(a)と同じである。また、ユーザのパスワードは、データベース4で管理されており、認証サービス部5がデータベース管理部6を通じて読み出す。

【0033】(S13) 認証処理部12は、データD4をそのままの状態ユーザ用コンピュータに送信する。

【0034】(S14) 認証要求部17aは、データD4をユーザのパスワードで復号化し、暗号鍵3とログイン証明書を取得する。

【0035】ここで、本発明のネットワークユーザ認証方法では、ネットワーク1の各資源に直接アクセスするのはユーザ用コンピュータ15ではなくゲートウェイコンピュータ11である。したがって、ネットワーク1の資源にアクセスするために必要なログイン証明書と暗号鍵3をゲートウェイコンピュータ11に渡す必要がある。このとき、ログイン証明書と暗号鍵3が第三者によって盗まれないためには暗号化する必要がある。そこで暗号化の鍵として、(S1)～(S10)で取得した暗号鍵2を使用することにした。以下(S15)～(S17)にその処理を示す。

【0036】(S15) 認証要求部17aは、暗号鍵D3とログイン証明書を(S10)で取得した暗号鍵D2で暗号化する。これをデータD5とする。

【0037】(S16) 認証要求部17aは、データD5をゲートウェイコンピュータ11へ送信する。

【0038】(S17) 認証処理部12は、データD5を暗号鍵D2で復号化し、暗号鍵D3とログイン証明書をパスワード管理テーブル13に登録する。ここで、暗号鍵D2を所有しているのは、ユーザ用コンピュータとゲートウェイコンピュータだけであるため、不正なコンピュータがデータD5を盗んでも復号化できない。

【0039】以上により、ネットワーク1へのログインが完了する。以後、ユーザがゲートウェイコンピュータを介してネットワーク1の資源へアクセスする場合、ゲートウェイコンピュータがユーザのログイン証明書をパスワード管理テーブル13から取り出して利用することとなる。

【0040】なお、上記の説明において、ゲートウェイコンピュータ11とサーバ14は別々のコンピュータであるが、両者は1台のコンピュータであっても良い。更にパスワード管理テーブル13において、図6に示すようなネットワーク1とネットワーク9におけるユーザのIDおよびパスワードの対応付けを管理し、ユーザがサ

サーバ14にログインすると認証処理部12がパスワード管理テーブル13からユーザのIDとパスワードを取り出してネットワーク1へのログイン処理を実行するように構成する。これにより、サーバ14とネットワーク1の両方にログインする場合でも、ユーザはサーバ14へのログイン操作だけで、ネットワーク1にもログインできる。ただし、ネットワーク1へのログインについては、ユーザが選択可能であってもよい。

【0041】また、同じくゲートウェイコンピュータ11とサーバ14を1台のコンピュータとした場合の例として、ゲートウェイコンピュータ11から管理コンピュータ5へのアクセスは、常にクライアント8を介して行うこととし、図2におけるゲートウェイコンピュータ11の処理をクライアント8が行い、ユーザ用コンピュータ15の処理をゲートウェイコンピュータ11が行うように構成しても良い。ネットワーク1におけるユーザのパスワードは、ゲートウェイコンピュータ11が図6に示すパスワード管理テーブルから読み出して使用する。この場合、実施例と同様にして不正なクライアント8を排除することができる。

【0042】他のシステム構成として、ゲートウェイコンピュータ11とクライアント8は1台のコンピュータであっても良い。また、ゲートウェイコンピュータ11とクライアント8およびサーバ14が1台のコンピュータであっても良い。

【0043】

【発明の効果】本発明は、各々独立に管理されるネットワークをゲートウェイコンピュータを介して相互に接続したネットワークシステムにおいて、不正なゲートウェイコンピュータを排除し、且つパスワードを通信媒体上に流さずにログインできるので、ユーザは各ネットワークのセキュリティレベルを損なうことなく、複数のネットワークの資源を利用することができる。

【0044】また本発明は、ユーザが一度の操作で複数のネットワークへログインできるので、複数のネットワークの資源を利用する場合でもユーザにとってログイン操作の負担が増えない。

【図面の簡単な説明】

【図1】本発明の実施例の統合ネットワークシステムのブロック図。

【図2】本発明の実施例の処理シーケンスを示す説明図。

【図3】図2における送信データの説明図。

【図4】図1におけるデータベース4に記録されるデータの例を示す説明図。

【図5】図1におけるパスワード管理テーブル13に記録されるデータの例を示す説明図。

【図6】本発明の実施例のパスワード管理テーブルに記録されるデータの一例を示す説明図。

【符号の説明】

11

12

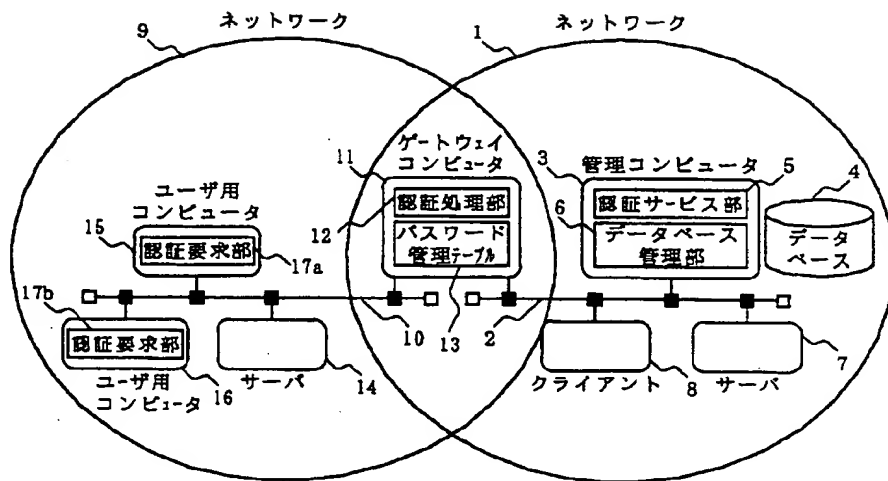
3...管理コンピュータ、

15...ユーザ用コンピュータ、

11...ゲートウェイコンピュータ、

【図1】

図1



【図3】

【図4】

図3

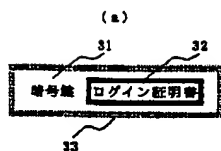
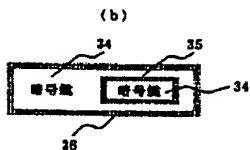


図4

ID	Password
GW_01	aaaa
user_A	xxx
user_B	yyy
user_C	www
...	...

【図5】

図5

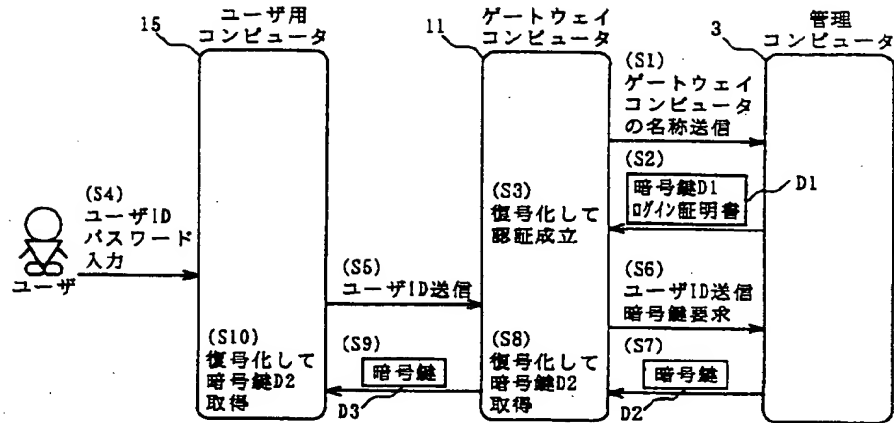


ネットワーク1の ID	ネットワーク1の Password	ログイン 証明書	暗号鍵
GW_01	aaaa	8000h	6000h
user_A	---	8032h	6008h
user_B	---	8064h	6016h
user_C	---	8096h	6024h
...

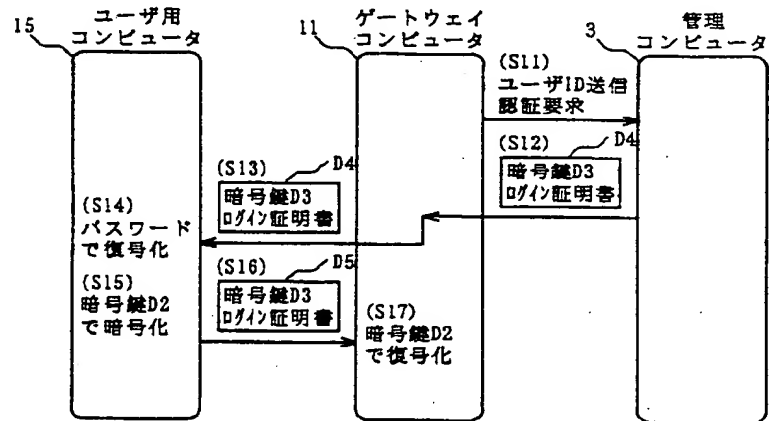
【図2】

図 2

(a)



(b)



【図6】

図6

13a

1719-12の ID	1719-12の Password	1719-11の ID	1719-11の Password	ログイン 証明書	暗号鍵
---	---	GW_01	aaa	8000h	6000h
USER_1	XX	user_A	xxx	8032h	6008h
USER_2	YYY	user_B	yyy	---	---
USER_3	ZZZ	user_C	zzz	8096h	6024h
...

フロントページの続き

(51)Int.Cl.6

H04L 9/32

識別記号

庁内整理番号

FI

技術表示箇所